

Best Available Copy



Europäisches
Patentamt

European
Patent Office

PCT/IB04

50956

Office européen
des brevets

REC'D 26 APR 2004

WIPO PCT

Bescheinigung Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03101092.9 ✓

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk



Anmeldung Nr:
Application no.: 03101092.9 ✓
Demande no:

Anmeldetag:
Date of filing: 18.04.03 ✓
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Secret identifier for renewed subscription

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s)
revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L29/06

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of
filing/Etats contractants désignés lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Secret identifier for renewed subscription

The invention relates to a method of secure device subscription, wherein a secret identifier and a public identifier are stored in a subscribing device, the subscribing device subscribes itself to a subscription authority, involving a step in which the subscribing device identifies itself with the public identifier, and a step in which the subscription authority supplies subscription information to the subscribing device.

5 The invention further relates to a subscription authority device, a subscribing device, a system, and a signal for secure device subscription.

10 In consumer applications, the production cost of a device is of utmost importance. Consequently, the ICs used in these applications preferably use standard and cheap process technology without any features like FLASH memory. A major problem then is that after a power-down of the device (such as when replacing the device's battery), any information not stored in ROM is lost. This is also true for the cryptographic information of a 15 device. Of course dedicated cryptographic information could be stored in ROM during production but this will in general make systems less flexible. If only the device's cryptographic identity is stored in ROM, the device has no way of proving its identity after power-down as this identity is public (it is used for addressing by other devices) and can therefore be spoofed by any other device.

20 Well-known public key infrastructure (PKI) technology uses therefore a pair of a public key and a private key. A device identifies itself with a public key, and it can prove to others with access to the public key that it is in possession of the corresponding private key without releasing that private key. Often, the public key is also used to address that device.

25 In some applications the overhead in terms of processing time and code size of the algorithms implementing the PKI technology is too large. An example of such an application is low-cost devices with wireless connections (sensors, home-security, building automation, remote metering, toys, mice, key boards, etc.) Every single device has a unique identifier stored in non-volatile memory (ROM). This identifier is used by other devices, directly or indirectly, for addressing purposes within a local network. Before a new device

(for example, just bought in a shop) can enter a (secured) network, it has to subscribe at a subscription authority which then acts as a Certifying Authority (CA). The CA and the device exchange subscription information in a (partially) secure environment. After this, the subscribing device can take part in the network communications. After power-down, the 5 device loses all subscription information and the CA has no way of verifying if the received identity is indeed the identity stored in the device. The only way out is to renew subscription to the network that is, in general, a time consuming and tedious process.

10 It is an object of the current invention to provide a method that enables the implementation of a low-cost and efficient subscription protocol, especially the protocol to renew subscription.

This object is realized by a method according to the invention characterized in that the method has a first-time subscription protocol and a renewed subscription protocol, 15 the subscription authority obtains a mapping of the secret identifier during the execution of the first-time subscription protocol, the subscription authority subsequently stores the mapping of the secret identifier, and the subscription authority uses the stored mapping of the secret identifier during the execution of the renewed subscription protocol.

The advantage of the invention is that devices no longer have to include non-volatile memory like FLASH or EEPROM which reduces device costs. By having the 20 subscription authority store a mapping of the secret identifier, that has been obtained during the execution of the first-time subscription protocol, a more efficient renewed subscription protocol can be executed when a subscribing device wants to renew its subscription, for example after a power down in which it lost its subscription information. The protocols are 25 therefore cheap and efficient to implement, and are often already available in these devices, as they often have at least some symmetric encryption algorithm implemented.

An embodiment of the method according to the invention is described in claim 2. In this embodiment of the invention both the subscription authority and the subscribing 30 device commonly and securely obtain a value r. This value is then encrypted by the subscribing device using the secret identifier, and subsequently communicated to the subscription authority. The value r can advantageously be applied during the renewed subscription. It can also advantageously be applied for other purposes, such as to store a backup of local information at the subscription authority, such that the local information remains available during or after the absence of a subscribing device, for example because of

a power down, or because the device is outside the range of the network. Another advantage of the usage of the value r is that the subscription authority doesn't learn anything about the secret identifier. When the subscribing device would subscribe to a different subscription authority in a different network, a different value r would be used and therefore the 5 subscriptions do not conflict with each other and the subscription authorities only have information relevant to their network.

An embodiment of the method according to the invention is described in claim 3. It describes how the subscription authority and subscribing device commonly and securely obtain a value r, namely, the subscription authority generates the value r, and 10 subsequently communicates it securely to the subscribing device.

An embodiment of the method according to the invention is described in claim 4. It describes how the subscription authority and subscribing device commonly and securely obtain a value r, namely, the subscription authority and the subscribing device together execute a protocol in order to arrive at a common secret value r.

15 An embodiment of the method according to the invention is described in claim 5. Both the first-time subscription protocol and the renewed subscription protocol are based on the communication from the subscription authority to the subscribing device of subscription information that is encrypted with the value r. Because this value r is only known to the subscription authority and the subscribing device, this communication does not 20 need to be secured.

An embodiment of the method according to the invention is described in claim 6. After a power down of the subscribing device, the value r is no longer available to the subscribing device. Therefore the subscription authority communicates the value r, encrypted with the secret identifier as encryption key. This way, the subscribing device with 25 the secret identifier can decrypt the communicated value and retrieve the value r, which it can then use further, for example to decrypt the communicated encrypted subscription information in the embodiment described in claim 5. Other devices than the subscribing device can not obtain the value of r, and the communication therefore does not need to be protected.

30 An embodiment of the method according to the invention is described in claim 7. The subscription authority stores the value r encrypted with the secret identifier as encryption key, which it needs during the execution of the renewed subscription protocol.

An embodiment of the method according to the invention is described in

claim 8. The subscription authority not only stores the encrypted the value r, but also the value r itself. This embodiment has the advantage that the subscription authority has access to the value r which it can use to encrypt and decrypt all kinds of information that is communicated to or from the subscribing device. Not only the subscription information, but 5 any information during execution of the subscription protocol or during normal operation can be secured in this way.

An embodiment of the method according to the invention is described in claim 9. In this embodiment of the invention the subscribing device securely communicates the secret identifier the subscription authority. The advantage of this embodiment is that it is-- 10 a very simple and therefore low-cost implementation of the invention.

An embodiment of the method according to the invention is described in claim 10. The subscription information is sent from the subscription authority to the subscribing device in encrypted form with the secret identifier as the encryption key. The advantage is that the symmetric key algorithm is efficient and low-cost.

15 An embodiment of the method according to the invention is described in claim 11. The subscription authority stores the secret identifier locally. The secret identifier can then be used during the execution of the renewed subscription protocol.

An embodiment of the method according to the invention is described in claim 12. The subscription information is communicated securely to the subscribing device 20 during execution of the first-time subscription protocol. The subscribing device encrypts the subscription information using the secret identifier as encryption key, and returns this information to the subscription authority. This embodiment has the advantage that the subscription authority can then use this encrypted subscription information during the execution of the renewed subscription protocol.

25 An embodiment of the method according to the invention is described in claim 13. The subscription authority communicates the subscription information, encrypted with the secret identifier of the subscribing device, to the subscribing device during the execution of the renewed subscription protocol.

An embodiment of the method according to the invention is described in 30 claim 14. The subscription authority stores the subscription information, encrypted with the secret identifier of the subscribing device. This enables the subscription authority to use this information during the execution of the renewed subscription protocol.

The subscription authority device according to the invention is characterized in that the subscription authority device is arranged to implement a first-time subscription

protocol, during which it receives a mapping of a secret identifier of a subscribing device, the subscription authority device is arranged to store the mapping of the secret identifier, the subscription authority device is further arranged to implement a renewed subscription protocol, during which it uses the stored mapping of the secret identifier.

- 5 The subscribing device according to the invention is characterized in that the subscribing device is arranged to contain a public identifier and a secret identifier, the subscribing device is further arranged to implement a first-time subscription protocol, during which it transmits a mapping of the secret identifier and during which it receives subscription information, the subscribing device is further arranged to implement a renewed subscription protocol, during which it receives subscription information which requires the secret identifier for decryption.
- 10 protocol, during which it receives subscription information which requires the secret identifier for decryption.

15 The system according to the invention is characterized in that it comprises a subscribing device as described in claim 16, and a subscription authority device as described in claim 15. The system according to the invention allows to build a secure and flexible system that allows renewed subscription of devices, even if the devices move between different networks or are repeatedly switched off and on.

20 The signal according to the invention is characterized in that the signal carries a mapping of a secret identifier of a subscribing device.

25 These and other aspects of the invention will be further described by way of example and with reference to the drawings, in which:

Fig. 1 illustrates a system with a first implementation of the first-time and renewed subscription protocols,

Fig. 2 illustrates a system with a second implementation of the first-time and renewed subscription protocols, and

Fig. 3 illustrates a system with a third implementation of the first-time and renewed subscription protocols.

30 Throughout the figures, same reference numerals indicate similar or corresponding features. Some of the features indicated in the drawings are typically implemented in software, and as such represent software entities, such as software modules or objects.

A first embodiment of the invention will be illustrated by the example shown in figure 1. Figure 1 shows an example of a system of (wireless) connected devices. System 100 contains a subscription authority 101 and a subscribing device 111. The subscribing device contains a public identifier 112 and a secret identifier 113. The first-time subscription protocol 120 illustrates on the hand of the communications symbolized between the subscription authority timeline 121 and the subscribing device timeline 122. During communication 130 the public identifier 112 is sent to the subscription authority in order to identify the subscribing device. Subsequently, the value r is sent to the subscribing device in secure communication 131. The value r can also be stored in memory 102 within the subscription authority device for later usage. This memory is preferably secured against tampering. A padlock in figure 1 symbolizes a secure connection. The connection can for example be secured by symmetric key encryption. The value r is then encrypted by the subscribing device using the secure identifier and communicated in step 132 to the subscription authority. The subscription authority 101 stores the encrypted value in its memory 102. Finally, the subscription authority encrypts the subscription information using the value r and sends this information in step 133 to the subscribing device.

A renewed subscription is more efficient than a first-time subscription. The renewed subscription 140 consists of the subscribing device identifying itself in step 150, after which the subscription authority transmits the value r , encrypted with the secret identifier, in step 151. This is a low-cost operation, as this value is already available in memory 102. Subsequently, the subscription authority transmits in step 152 the subscription information, encrypted using the value r . This information could have been stored in memory 102 or can be recomputed. The subscribing device retrieves the value r using its secret identifier, and then retrieves the subscription information.

The secure authenticated channel in step 131 can be for example a cryptographically secure channel, or a physically secure channel where no eavesdropping is possible (for a physically secured channel one could think of a Faraday room, near-field communication, or reduced power radio communication).

For the invention it is not required that the subscription authority and subscribing device share common secret information, and instead of communicating the common value r it can also be obtained for example by using algorithms like Diffie-Hellman key establishment or Shamir's no-key protocol (see Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, p515 and p499, respectively) to generate a common value r .

This protocol is safe from an attack from a pseudo-subscription authority, pretending to be a subscription authority, in order to obtain information to impersonate a subscribing device or to retrieve sufficient information to successfully eavesdrop on the communication. Practically, it would be possible to remove the batteries from the subscribing device, replace the batteries and initiate a subscription protocol with a pseudo-subscription authority. But because the value r is chosen by the subscription authority, the pseudo-subscription authority does not learn sufficient information to compromise the communication between subscription authority and subscribing device.

Figure 2 shows a second embodiment of the invention. During the execution of the first-time subscription protocol, the subscribing device reveals its public identity in step 230. In step 231 the secret identifier is communicated securely to the subscription authority as well. Subsequently, the subscription authority encrypts the subscription information using the secret identifier and communicates the encrypted subscription information to the subscribing device in step 232.

The renewed subscription is even simpler, as it consists of only two steps (step 251 and 252 optional). In step 250 the subscribing device identifies itself, and in step 253 the subscription authority communicates the encrypted subscription information to the subscribing device. The encrypted subscription information can be obtained from storage 102 (if it does not change) or it can be recomputed (if the subscription information has changed) by encrypting it using the secret identifier. The subscribing device can decrypt this information using its secret identifier. The authorization is implicit: only the subscribing device with access to the secret identifier can obtain the subscription information.

It can also do explicit authentication by starting a challenge response-protocol of which a simple version is described here but any symmetric key based challenge-response will do. In this simple version, step 251 may communicate the value r encrypted using the secret identifier to the device as a challenge, and the subscribing device should return the value r to the subscription authority in step 252. Failing that, the subscription authority will refuse the subscribing device.

Figure 3 shows a third embodiment of the invention. During the execution of the first-time subscription protocol, the subscribing device reveals its public identity in step 330. In step 331 the subscription information is communicated securely from the subscription authority to the subscribing device. Subsequently, the subscribing device encrypts the subscription information using the secret identifier and communicates the encrypted subscription information to the subscription authority in step 332.

This embodiment has the advantage that the secret identifier does not leave the subscribing device.

The renewed subscription is as simple as in the previous embodiment. In step 350 the subscribing device identifies itself, and in step 351 the subscription authority 5 communicates the stored encrypted subscription information to the subscribing device. The subscribing device can decrypt this information using its secret identifier. The authorization is implicit: only the subscribing device with access to the secret identifier can obtain the subscription information.

Alternatives are possible. In the description above, "comprising" does not 10 exclude other elements or steps, "a" or "an" does not exclude a plurality, and a single processor or other unit may also fulfill the functions of several means recited in the claims. Actual communication includes the actual communication between different devices or parts 15 of a device, by means of optical, electronic, wireless, microwave, or any other suitable technology, or even communication between software components within a processing system or between processing systems.

CLAIMS:

1. A method of secure device subscription, wherein
a secret identifier and a public identifier are stored in a subscribing device,
the subscribing device subscribes itself to a subscription authority, involving
a step in which the subscribing device identifies itself with the public
5 identifier, and
a step in which the subscription authority supplies subscription
information to the subscribing device,
characterized in that
the method has a first-time subscription protocol and a renewed subscription
10 protocol,
the subscription authority obtains a mapping of the secret identifier during
execution of the first-time subscription protocol,
the subscription authority subsequently stores the mapping of the secret
identifier, and
15 the subscription authority uses the stored mapping of the secret identifier
during execution of the renewed subscription protocol.
2. The method according to claim 1, wherein during execution of the first-time
subscription protocol
20 the subscription authority and subscribing device commonly and securely
obtain a value r,
the subscribing device subsequently encrypts the value r using the secret
identifier as encryption key, and
the subscribing device subsequently communicates the encrypted value to the
25 subscription authority.
3. The method according to claim 2, wherein during execution of the first-time
subscription protocol
the subscription authority generates the value r, and

the subscription authority communicates the value r securely to the subscribing device.

4. The method according to claim 2, wherein during execution of the first-time
5 subscription protocol the subscription authority and subscribing device commonly generate a
value r using a secure common key generation protocol.

5. The method according to claim 2, wherein during execution of any of the
subscription protocols

10 the subscription authority encrypts the subscription information using the
value r as encryption key, and
the subscription authority subsequently communicates the encrypted
subscription information to the subscribing device.

15 6. The method according to claim 2, wherein during execution of the renewed
subscription protocol the subscription authority communicates the value r encrypted with the
secret identifier as encryption key to the subscribing device.

7. The method according to claim 2, wherein the stored mapping of the secret
20 identifier is the value r, encrypted with the secret identifier as encryption key.

8. The method according to claim 7, wherein the value r is also stored by the
subscription authority.

25 9. The method according to claim 1, wherein during execution of the first-time
subscription protocol the subscribing device communicates the secret identifier to the
subscription authority.

10. The method according to claim 1, wherein during execution of any of the
30 subscription protocols
the subscription authority encrypts the subscription information using the
secret identifier, and
the subscription authority subsequently communicates the encrypted
subscription information to the subscribing device.

11. The method according to claim 1, wherein the stored mapping of the secret identifier is the secret identifier itself.
- 5 12. The method according to claim 1, wherein during execution of the first-time subscription protocol
 - the subscription authority communicates the subscription information securely to the subscribing device,
 - the subscribing device subsequently encrypts the subscription information
- 10 using the secret identifier as encryption key, and
 - the subscribing device subsequently communicates the encrypted subscription information to the subscription authority.
13. The method according to claim 1, wherein during execution of the renewed subscription protocol the subscription authority communicates the encrypted subscription information to the subscribing device.
- 15 14. The method according to claim 1, wherein the stored mapping of the secret identifier is the subscription information encrypted with the secret identifier as encryption key.
- 20 15. A subscription authority device for secure device subscription, characterized in that
 - the subscription authority device is arranged to implement a first-time subscription protocol, during which it receives a mapping of a secret identifier of a subscribing device,
 - the subscription authority device is arranged to store the mapping of the secret identifier,
 - the subscription authority device is further arranged to implement a renewed subscription protocol, during which it uses the stored mapping of the secret identifier.
- 30 16. A subscribing device to participate in a network requiring subscription, characterized in that

the subscribing device is arranged to contain a public identifier and a secret identifier,

the subscribing device is further arranged to implement a first-time subscription protocol,

5 during which it transmits a mapping of the secret identifier and during which it receives subscription information,

the subscribing device is further arranged to implement a renewed subscription protocol,

10 during which it receives subscription information which requires the secret identifier for decryption.

17. A system for secure device subscription, the system comprising a subscribing device is described in claim 16, and a subscription authority device is described in claim 15.

15

18. A signal for secure device subscription, characterized in that the signal carries a mapping of a secret identifier of a subscribing device.

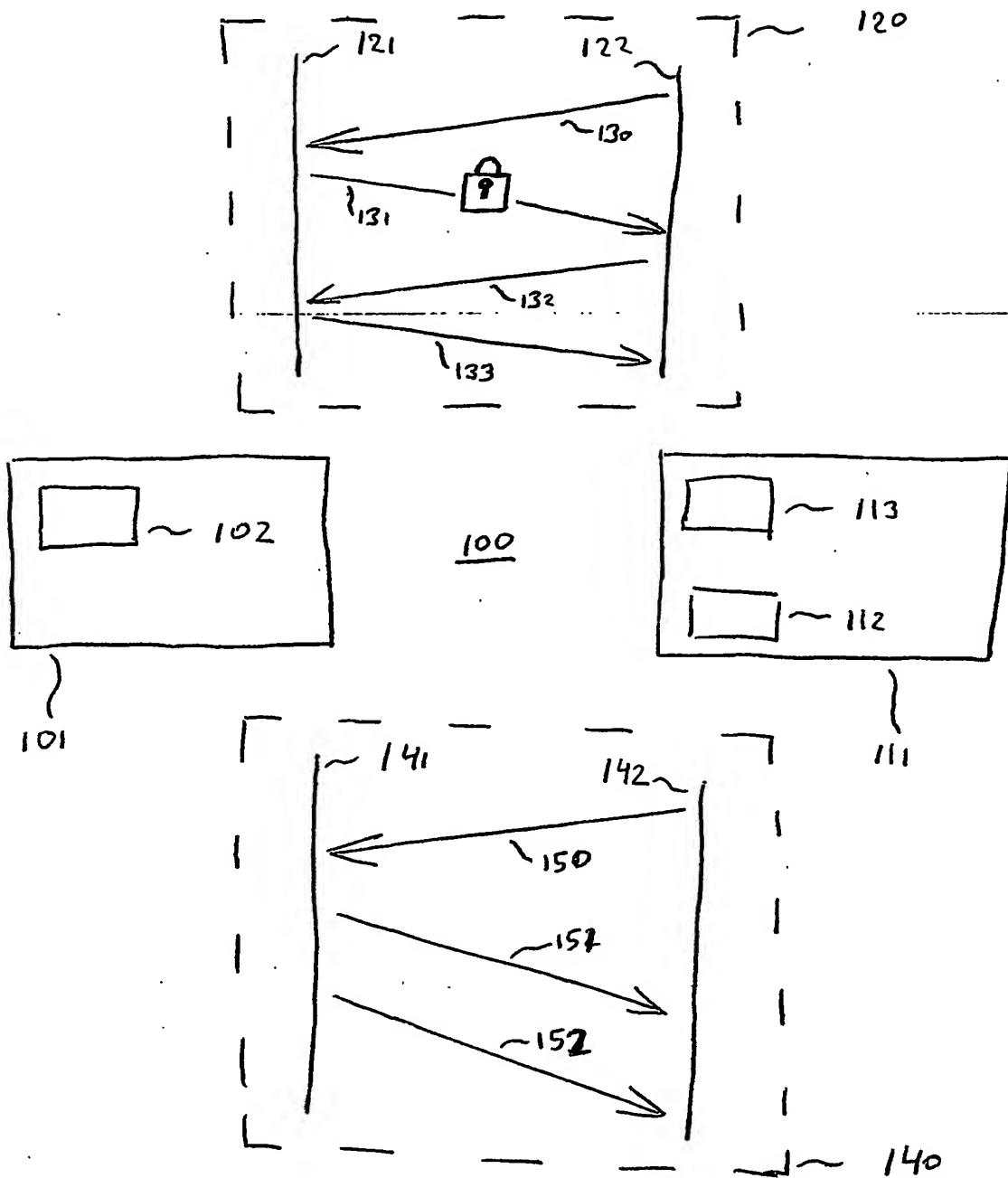
ABSTRACT:

The invention relates to cryptographic identification in a practical, low cost environment. A secret number (a kind of hidden identity) is stored in a device that, in combination with its public identity, can be used for identification by a Certifying Authority (CA) and subsequent subscription. To enable efficient renewed subscription, the CA will store a mapping of the hidden identity.

5 Fig. 1

HNL030457

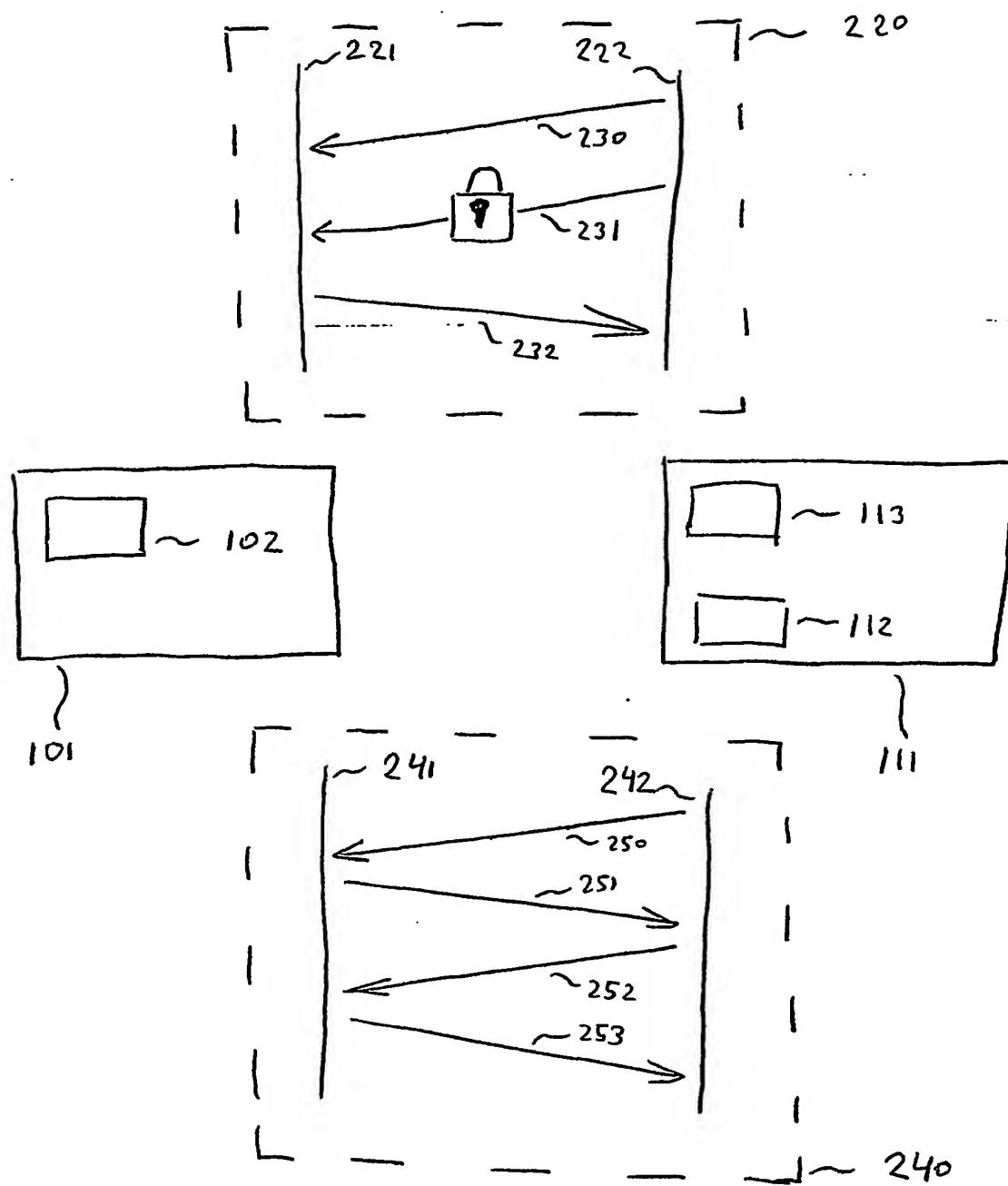
1/3



Eig. 1

DHN1030457

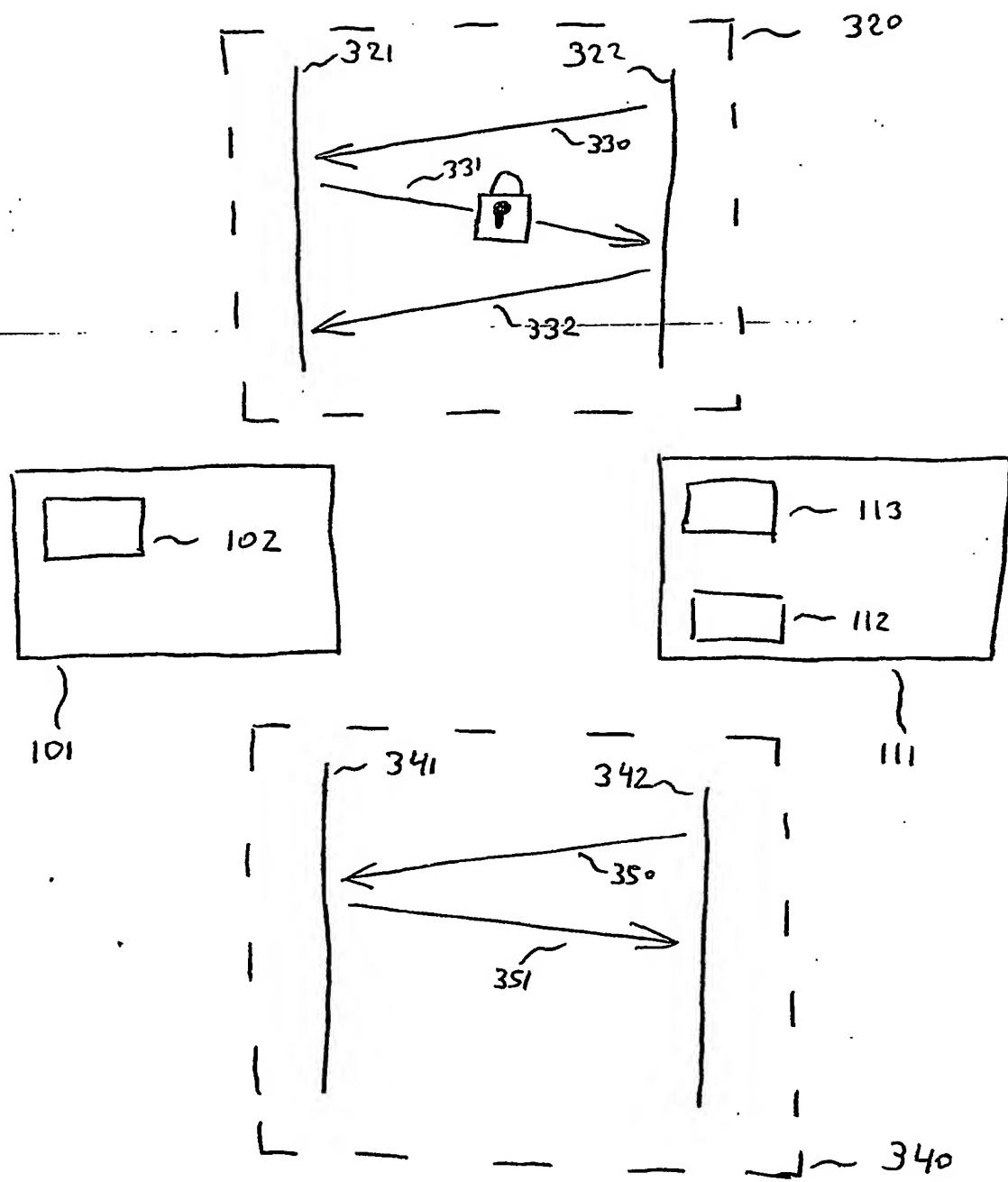
2/3



Eig. 2

0HN1030457

3/3



Eig. 3

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

FADED TEXT OR DRAWING

BLURRED OR ILLEGIBLE TEXT OR DRAWING

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.